PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 20 April 2000 (20.04.00)	
International application No.: PCT/EP99/07052	Applicant's or agent's file reference: P98135WO.1P
International filing date: 22 September 1999 (22.09.99)	Priority date: 09 October 1998 (09.10.98)
Applicant: SCHWENK, Jörg	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

12 February 2000 (12.02.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: ANMELDEAMT

PCT

An
DEUTSCHE TELEKOM AG
Patentabteilung R151
D-64307 Darmstadt
ALLEMAGNE

MITTEILUNG DES INTERNATIONALEN AKTENZEICHENS UND DES INTERNATIONALEN ANMELDEDATUMS

(Regel 20.5.c) PCT)

Absendedatum (*Tag/Monat/Jahr*)	01. 11. 99
Aktenzeichen des Anmelders oder Anwalts: P98135WO.1P	WICHTIGE MITTEILUNG

Internationales Aktenzeichen	Internationales Anmeldedatum (*Tag/Monat/Jahr*)	Prioritätsdatum (*Tag/Monat/Jahr*)
PCT/EP 99/07052	22/09/1999	09/10/1998

Anmelder: DEUTSCHE TELEKOM AG

Bezeichnung der Erfindung:

1. Dem Anmelder wird mitgeteilt, daß der internationalen Anmeldung das oben genannte internationale Aktenzeichen und internationale Anmeldedatum zuerkannt worden ist.
2. Weiterhin wird dem Anmelder mitgeteilt, daß das Aktenexamplar der internationalen Anmeldung dem Internationalen Büro am oben angegebenen Absendedatum übermittelt worden ist.
3. ☐ Sonstiges:

* Das Internationale Büro überwacht die Übermittlung des Aktenexemplars durch das Anmeldeamt und unterrichtet den Anmelder über dessen Eingang (mit Formblatt PCT/IB/301). Ist das Aktenexemplar bei Ablauf des vierzehnten Monats nach dem Prioritätsdatum noch nicht eingegangen, teilt das Internationale Büro dies dem Anmelder mit (Regel 22.1.c)).

Name und Postanschrift des Anmeldeamts	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	R.L.R. Pether

Formblatt PCT/RO/105 (0792) P20404

09/807,176
Translation
SOCO

3

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P98135WO.1P	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP99/07052	International filing date (*day/month/year*) 22 September 1999 (22.09.99)	Priority date (*day/month/year*) 09 October 1998 (09.10.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant DEUTSCHE TELEKOM AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12 February 2000 (12.02.00)	05 October 2000 (05.10.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/07052

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☒ the international application as originally filed.

☒ the description, pages 1,2, as originally filed,
pages _____, filed with the demand,
pages 3,3a,4,5, filed with the letter of 08 August 2000 (08.08.2000),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1, filed with the letter of 08 August 2000 (08.08.2000),
Nos. _____, filed with the letter of _____.

☐ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1	YES
	Claims		NO
Inventive step (IS)	Claims	1	YES
	Claims		NO
Industrial applicability (IA)	Claims	1	YES
	Claims		NO

2. Citations and explanations

1. This report makes reference to the following documents:

D1 IEEE Infocom '93. The conference on computer communications proceedings. Twelfth annual joint conference of the IEEE computer and communications societies. Networking: Foundation for the future (cat. No.93CH3264-9) (28-03-1993), Vol. 3, pages 1406-1413. "On the design of conference key distribution systems for the broadcasting networks".

2. D1, mentioned on page 3 of the description, discloses (page 1409, column 2, last paragraph to page 1410, column 1) a method for establishing a common key between an exchange (chairman) and a group of n subscribers. Shares are derived and the (n+1.2n) threshold method of D1 is equivalent to (n, 2n-1) threshold method of Claim 1.

Even in D1 the exchange does not have to know the secret key of the subscribers; only one common key is required between the subscribers and the exchange (see D1, page 1410, column 1, paragraph 1), which, for example could be formed in a known manner (see

page 1 of the application) from the secret key of the subscriber and the exchange without the exchange having to know the key of the subscriber.

3. As a result the method of the present claim differs from the disclosure of D1 in that the common key is determined by contributions of all group members. The risk of a weak key is therefore excluded to a large degree.

4. The search report citations do not disclose or suggest such a procedure. Consequently, the subject matter of the claim can be regarded as novel and inventive (PCT Article 33(3)).

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
P98135WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/07052	22/09/1999	09/10/1998
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK		
H04L9/08		
Anmelder		
DEUTSCHE TELEKOM AG ET AL		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 4 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 5 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
12/02/2000	05.10.2000
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Zucka, G Tel. Nr. +31 70 340 4026

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/07052

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1,2	ursprüngliche Fassung			
3,3a,4,5	eingegangen am	28/08/2000	mit Schreiben vom	08/08/2000

Patentansprüche, Nr.:

1	eingegangen am	28/08/2000	mit Schreiben vom	08/08/2000

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

Zu Punkt V

1. Es wird auf das folgende Dokument verwiesen:

   D1 = IEEE Infocom ' 93. The Conference On Computer Communications Proceedings. Twelfth Annual Joint Conference Of The IEEE Computer And Communications Societies. Networking: Foundation For The Future (cat. No.93CH3264-9) (28-03-1993), Vol.3, Seiten 1406-1413, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks"

2. Das Dokument D1, das auf Seite 3 der Beschreibung erwähnt wird, offenbart (Seite 1409, Spalte 2, letzter Absatz - Seite 1410, Spalte 1) ein Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale (chairman) und einer Gruppe von n Teilnehmern. Es werden shares abgeleitet, und das (n+1,2n)-Threshold-Verfahren von D1 ist äquivalent zum (n,2n-1)-Threshold-Verfahren des Anspruchs 1.

   Auch in D1 muß die Zentrale die geheimen Schlüssel der Teilnehmer nicht kennen; es wird lediglich ein gemeinsamer Schlüssel zwischen Teilnehmer und Zentrale benötigt (siehe D1, Seite 1410, Spalte 1, Absatz 1), der z.B. auf bekannter Weise (siehe Seite 1 der Anmeldung) aus den geheimen Schlüssel des Teilnehmers und der Zentrale gebildet werden könnte, ohne daß die Zentrale den Schlüssel des Teilnehmers kennen muß.

3. Das Verfahren vom vorliegenden Anspruch unterscheidet sich dadurch von der Offenbarung des Dokuments D1, daß der gemeinsame Schlüssel aus den Beiträgen aller Gruppenmitglieder ermittelt wird. Das Risiko eines schwachen Schlüssels wird somit weitgehend ausgeschlossen.

4. Eine solche Vorgehensweise wird von den im Recherchenbericht zitierten Dokumenten weder offenbart noch nahegelegt. Der Gegenstand des Anspruchs wird deshalb als neu und erfinderisch betrachtet (Artikel 33.3 PCT).

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000Bit gesendet werden müssen.

Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptographisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

In IEEE Infocom `93. The Conference On Computer Communications Proceedings. Twelth Annual Joint Conference Of The IEEE Computer And Communications Societies. Networking: Foundation For The Future (cat. No.93CH3264-9) (28-03-1993), Vol.3, Seiten 1406-1413, „On the Design of Conference Key Distribution Systems for the Broadcasting Networks" wird ein Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale (chairman) und einer Gruppe von n Teilnehmern beschrieben, bei dem ein Threshold-Verfahren zum Einsatz kommt. Bei dieser Lösung wählt die Zentrale (chairman) einen gemeinsamen Schlüssel. Das Verfahren setzt einen sicheren Kanal zwischen dem chairman und den Teilnehmern voraus. Ein solcher sicherer Kanal kann z.B. mit dem oben angeführten DH-Verfahren [DH76] oder einer Variante etabliert werden. Pro Teilnehmer sind dazu jedoch zwei Nachrichten erforderlich, um zwischen den n Teilnehmern und der Zentrale (chairman) einen gemeinsamen Schlüssel auszuhandeln und eine Nachricht um die „public shadows zu senden.

Damit sind zum Etablieren des gemeinsamen Schlüssels insgesamt 2n+1 Nachrichten erforderlich.

Das vorliegende Verfahren zur Erzeugung eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von mindestens drei Teilnehmern soll den gleichen Sicherheitsstandard wie das DH-Verfahren aufweisen. Das Verfahren soll dabei jedoch einfach zu implementieren sein und einen minimalen Rechenaufwand benötigen.

Das erfindungsgemäße Verfahren, das dieser Aufgabenstellung gerecht wird, basiert auf den gleichen mathematischen Strukturen, wie das DH-Verfahren und weist daher vergleichbare Sicherheitsmerkmale auf. Im Vergleich zu den bisher vorgeschlagenen Gruppen-DH-Verfahren ist es wesentlich effizienter im Hinblick auf Rechenaufwand und Kommunikationsbedarf.

Nachfolgend wird das Wirkprinzip des erfindungsgemäßen Verfahrens näher erläutert. Die Zentrale wird dabei mit Z bezeichnet, definierte Teilnehmer am Verfahren mit T1-Tn und jeder einzelne nicht konkret benannte Teilnehmer mit Ti. Die öffentlich bekannten Komponenten des Verfahrens sind eine öffentlich bekannte mathematische Gruppe G,

vorzugsweise die multiplikative Gruppe aller ganzen Zahlen modulo einer großen Primzahl p, und ein Element g der Gruppe G, vorzugsweise eine Zahl $0<g<p$ mit großer multiplikativer Ordnung. Für die Gruppe G können jedoch auch andere geeignete mathematische Strukturen verwendet werden, z.B. die multiplikative Gruppe eines endlichen Körpers, oder die Gruppe der Punkte einer elliptischen Kurve.

Das Verfahren verläuft in drei Arbeitsschritten.

Im ersten Arbeitsschritt wird von jedem Teilnehmer Ti eine Nachricht der Form (Ti, g^i mod p) an die Zentrale gesendet, wobei i eine mittels eines Zufallsgenerators gewählte zufällige Zahl des Teilnehmers Ti ist.

Im zweiten Arbeitsschritt wird in der Zentrale Z

- eine zufällige Zahl z generiert und für jeden Teilnehmer Ti die Zahl $(g^i)^z$ mod p berechnet.
- Bei n Teilnehmern werden in der Zentrale Z dann aus diesen n Zahlen n shares mit Hilfe eines an sich bekannten (n,2n-1) Threshold Verfahrens abgeleitet.
- In der Zentrale Z werden n-1 weitere shares s^1-s^{n-1} ausgewählt und zusammen mit der Zahl g^z mod p an alle Teilnehmer T1-Tn gesendet.

Im dritten Arbeitsschritt wird bei jedem Teilnehmer Ti der gemeinsamen Schlüssel k berechnet, wobei

- $(g^z)^i$ mod p = $(g^i)^z$ mod p berechnet wird,
- daraus ein share des Threshold Verfahrens abgeleitet wird und
- mit diesem share und $s^1,...s^{n-1}$ als Geheimnis der gemeinsame Schlüssel k ermittelt wird.

Nachfolgend wird das erfindungsgemäße Verfahren anhand eines konkreten Beispiels für drei Teilnehmer A, B, und C sowie einer Zentrale Z näher erläutert. Die Anzahl der Teilnehmer ist jedoch auf beliebig viele Teilnehmer erweiterbar.

Bei diesem Beispiel beträgt die Länge der Zahl p 1024 Bit; g hat eine multiplikative Ordnung von mindestens 2^{160}.

Das erfindungsgemäße Verfahren läuft nach folgenden Verfahrensschritten ab:

1. Teilnehmer A, B und C senden g^a mod p, g^b mod p und g^c mod p an die Zentrale Z.
2. In der Zentrale Z wird g^{az} mod p, g^{bz} mod p und g^{cz} mod p berechnet, wobei jeweils die 128 Least Significant Bits davon als shares s_A, s_B bzw. s_C verwendet werden. In der Zentrale Z wird mittels des (n,2n-1)-Threshold-Verfahrens ein Polynom P(x) über einem endlichen Körper GF(2^{128}) vom Grad 2 berechnet, das durch die Punkte (1,s_A), (2,s_B) und (3,s_C) geht und durch diese eindeutig festgelegt ist. Der gemeinsame Schlüssel k ist der Schnittpunkt dieses Polynoms mit der y-Achse, d. h. k; =P(0). Die Zentrale Z sendet nun g^z mod p, s_1;=P(4) und s_2;=P(5) an die Teilnehmer A, B und C.
3. Beim Teilnehmer A wird $(g^z)^a$ mod p berechnet. Im Ergebnis erhält der Teilnehmer A mit den 128 Least Significant Bits dieses Wertes den share s_A, der zusammen mit den shares s_1 und s_2 ausreicht, das Polynom P'(x) und damit auch den Schlüssel k zu bestimmen. Bei den Teilnehmern B und C wird analog verfahren.

Das oben beschriebene Verfahren kommt mit der minimalen Anzahl von zwei Runden zwischen den Teilnehmern T1-Tn und Zentrale Z aus. In der zweiten Runde kann der Aufwand für die von der Zentrale an die n Teilnehmer zu übertragenden Zeichenfolgen im Gegensatz zu der Lösung von Burmester und Desmedt auf eine Länge von jeweils 128 Bit pro Teilnehmer reduziert werden.

(1) Patentanspruch:

1. Verfahren zum Etablieren eines gemeinsamen Schlüssels k zwischen einer Zentrale Z und einer Gruppe von Teilnehmern T1-Tn mit einer öffentlich bekannten mathematischen Gruppe G und einem Element $g \in G$ von großer Ordnung in der Gruppe G, so daß für die Gruppe G und das Element g die Berechnung des diskreten Logarithmus praktisch unmöglich ist, und unter Verwendung eines an sich bekannten Threshold-Verfahrens, **dadurch gekennzeichnet**, daß

a) von jedem Teilnehmer Ti eine Zufallszahl i generiert und aus dem bekannten Element $g \in G$ und der jeweiligen Zufallszahl i von jedem Teilnehmer Ti der Wert g^i berechnet und zur Zentrale Z gesendet wird, daß

b) in der Zentrale Z eine Zufallszahl z generiert wird, daß aus der Zufallszahl z und den empfangenen Werten g^i die Werte $(g^i)^z$ in G berechnet werden, daß aus diesen Werten n shares $(s_1,...,s_n)$ des Threshold-Verfahrens abgeleitet werden , und daß aus den shares $(s_1,...,s_n)$ das (n,2n-1)-Threshold-Verfahren konstruiert wird, wobei das durch dieses Verfahren implizid gegebene Geheimnis der zu etablierende Schlüssel k ist, daß in der Zentrale Z n-1 weitere, von den shares $(s_1,...,s_n)$ verschiedene shares $(s_{n+1},...s_{2n-1})$ zusammen mit dem Wert g^z in G berechnet und an die Teilnehmer T1-Tn übertragen werden, und daß

c) bei jedem Teilnehmer Ti der zu etablierende Schlüssel k dadurch rekonstruiert wird, daß aus dem von der Zentrale Z übertragenen Wert g^z und der Zufallszahl i des jeweiligen Teilnehmers Ti der Wert für $(g^z)^i$ in G berechnet wird, daß aus dem resultierenden Wert mittels des Threshold Verfahrens der share s_i abgeleitet wird und daß mit dem share s_i und den von der Zentrale Z übertragenen shares $(s_{n+1},...s_{2n-1})$ mit Hilfe des (n,2n-1)-Threshold-Verfahrens der Schlüssel k rekonstruiert wird.

Revised pages (German pages 3, 3a, 4, 5, 6)

Another method for establishing a common key is known from the German Patent DE 195 38 385.0. In this method, however, the central station must know the secret keys of the subscribers.

An approach is also known from Burmester, Desmedt, "A Secure and Efficient Conference Key Distribution System", Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994, where two rounds are required to generate the key, it being necessary to send n communications of a length of p = approx. 1000 bits through the central station for n subscribers in the second round. A cryptographic method described as the (n,t) threshold method is also known. In an (n,t) threshold method, a key k can be decomposed into t parts (referred to as shadows), in such a way that this key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Publishers, Wiesbaden, 1998).

In IEEE Infocom '93, The Conference on Computer Communications Proceedings, Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies, Networking: Foundation for the Future (cat. no. 93CH3264-9) (3/28/1993), vol. 3, pp. 1406-1413, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks", a method is described for establishing a common key between a central station (chairman) and a group of n subscribers, where a threshold method is employed. In this approach, the central station (chairman) selects a common key. The method presupposes a secure channel between the chairman and the subscribers. A secure channel of this kind can be established, for example, using the DH method [DH76] indicated above, or a variant. However, for this, two communications are necessary for each subscriber, in order to negotiate a common key between the n subscribers and the central station (chairman), and to transmit a communication around the "public shadows".

Thus, altogether 2n+1 communications are required in order to establish the common key.

It is intended that the present method for generating a common key between a central station and a group of at least three subscribers have the same security standards as the DH method. In this context, however, the method should be simple to implement and require minimal computational outlay.

The method according to the present invention is equal to this task. It is based on the same mathematical structures as the DH method and, therefore, has comparable security features. In comparison to the group DH methods proposed in known methods heretofore, it is substantially more efficient with respect to computational outlay and communication requirements.

The operating principle of the method according to the present invention is elucidated in the following. In this instance, the central station is denoted by Z, defined subscribers in the method by T1-Tn, and every single subscriber, who is not specifically named, by Ti. The publicly known components of the method include a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of the group G, preferably a number $0<g<p$ having a high multiplicative order. For group G, however, other suitable mathematical structures can also be used, e.g., the multiplicative group of a finite field, or the group of the points of an elliptical curve.

The method is carried out in three work steps.
In the first step, a communication in the form (Ti, g^i mod p) is sent by each subscriber Ti to the central station, i being a random number of subscriber Ti selected by a random number generator.

In the second work step, in central station Z:

- A random number z is generated, and the number $(g^i)^z$ mod p is calculated for each subscriber Ti.
- From these n numbers, n shares are then differentiated for n subscribers in central station Z, using a generally known (n, 2n-1) threshold method.
- n-1 further shares s^1-s^{n-1} are selected in central station Z and sent, together with the number g^z mod p, to all subscribers Tl-Tn.

In the third work step, the common key k is calculated for each subscriber Ti,- $(g^z)^i$ mod p = $(g^i)^z$ mod p being calculated;

- from this, a share of the threshold method being differentiated; and
- on the basis of this share and $s^1,...s^{n-1}$, common key k being determined as the secret.

On the basis of a practical example, the method according to the present invention is elucidated in the following for three subscribers A, B, and C, as well as a central station Z. However, the number of subscribers can be increased to any desired number. In this example, the length of number p is 1024 bits; g has a multiplicative order of at least 2^{160}.

The method in accordance with the present invention is carried out in accordance with the following method steps:

1. Subscribers A, B and C send g^a mod p, g^b mod p and g^c mod p to central station Z.
2. g^{az} mod p, g^{bz} mod p and g^{cz} mod p are calculated in central station Z, in each case the 128 least significant bits thereof being used as shares S_A, S_B and, respectively, S_C. In central station Z, applying the (n,2,-1) threshold method, a 2nd degree polynomial P(x), which passes through points $(1,s_A)$, $(2,s_B)$, and $(3,s_C)$ and is uniquely defined by these points, is calculated over a finite field $GF(2^{128})$. Common key k is the point of intersection of this polynomial with the y-axis, i.e., k; =P(0). Central

station Z transmits g^z mod p, s_1;=P(4) and s_2;=P(5) to subscribers A, B and C.

3. For subscriber A, $(g^z)^a$ mod p is calculated. In the result, subscriber A having the 128 least significant bits of this value receives share s_A, which, together with shares s_1 and s_2 is sufficient to determine polynomial P'(x) and, thus, also key k. One proceeds analogously for subscribers B and C.

The method described above makes do with the minimum number of two rounds between subscribers T1-Tn and central station Z. In contrast to the Burmester and Desmedt approach, the outlay for character strings to be transmitted by the central station to the n subscribers can be reduced in the second round to a length of 128 bits per subscriber.

What is claimed is:

1. A method for establishing a common key k between a central station Z and a group of subscribers T1-Tn, comprising a publicly known mathematical group G and an element $g \in G$ of a high order in the group G, so that for group G and the element g, the calculation of the discrete logarithm is virtually impossible, and with the use of a generally known threshold method,
wherein

a) a random number i is generated by each subscriber Ti and, from the known element $g \in G$ and the random number i in question, the value g^i is calculated by each subscriber Ti and transmitted to the central station Z;

b) in the central station Z, a random number z is generated; from the random number z and the received values g^i, the values $(g^i)^z$ in G are calculated; from these values, n shares $(s_1,\ldots,s_n)$ of the threshold method are derived; and
from the shares $(s_1,\ldots,s_n)$, the (n,2n-1) threshold method is constructed, the secret implicitly given by this method being the key k to be established;
in the central station Z, n-1 further shares $(s_{n+1},\ldots s_{2n-1})$ differing from shares $(s_1,\ldots,s_n)$ are calculated, together with the value g^z in G, and transmitted to the subscribers T1-Tn; and

c) for each subscriber Ti, the key k to be established is reconstructed in that, from the value g^z transmitted by the central station Z, and the random number i of the subscriber Ti in question, the value for $(g^z)^i$ in G is calculated; that from the resulting value, applying the threshold method, the share s_i is derived, and that, on the basis of the share s_i and the shares $(s_{n+1},\ldots s_{2n-1})$ transmitted by the central

station Z, the key k is reconstructed with the aid of the (n,2n-1) threshold method.

PROVISIONAL INTERNATIONAL EXAMINATION REPORT

International Reference no. PCT/EP99/07052

1. Basis for the Report

2. This report was prepared on the basis of (substitute pages submitted to the Receiving Office in response to a request according to Article 14, are considered as "originally filed" within the framework of this report, and are not enclosed with the report because they do not contain any amendments.):

Specification, pages:

1,2 original version
3,3a,4,5 filed on 8/28/2000 with letter of 8/8/2000

Patent Claims, no.

1 filed on 8/28/2000 with letter of 8/8/2000

V. Substantiated determination pursuant to Article 35(2) with respect to novelty, inventive activity, and industrial applicability; documents and clarifications in support of this determination

1. Determination

Novelty (N)	Yes:	Claims 1
	No:	Claims
Inventive Activity (ET)	Yes:	Claims 1
	No:	Claims
Industrial Applicability (GA)	Yes:	Claims 1
	No:	Claims

2. Documents and Clarifications
see enclosure

With respect to Point V

1. Reference is made to the following document:

D1 = IEEE Infocom '93. The Conference on Computer Communications Proceedings. Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies. Networking: Foundation for the Future (cat. no. 93CH3264-9) (3/28/1993), vol. 3, pp. 1406-1413, "On the Design of Conference Key Distribution Systems for the Broadcasting Networks"

2. Document D1, referred to on page 3 of the Specification, discloses (page 1409, column 2, last paragraph - page 1410, column 1) a method for establishing a common key between a central station (chairman) and a group of n subscribers. Shares are derived, and the (n+1,2n) threshold method of D1 is equivalent to the (n,2n-1) threshold method of Claim 1.

In D1 as well, it is not necessary for the central station to know the secret keys of the subscribers; a common key between the subscribers and the central station is merely required (see D1, page 1410, column 1, paragraph 1), which, for example, in a generally known way (see page 1 of the Application), could be generated from the secret key of the subscriber and the central station, without it be necessary for the central station to know the key of the subscriber.

- The method of the present claim is thereby distinguished from the disclosure of document D1 in that the secret key is determined from the contributions of all group members. This substantially rules out the risk of a weak key.

- A procedure of this kind is neither disclosed nor anticipated by any of the documents cited in the Search Report. The subject matter of the claim is, therefore, considered to be novel and inventive (Article 33.3 PCT).

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen: PCT/EP 99/07052

Internationales Anmeldedatum: (22.09.1999) 22 SEP 1999

EUROPEAN PATENT OFFICE
PCT INTERNATIONAL APPLICATION
Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)*: P98135WO.1P

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

DEUTSCHE TELEKOM AG
Friedrich-Ebert-Allee 140

53113 Bonn
Deutschland

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

SCHWENK; Jörg
Südwestring 27

64807 Dieburg
DE

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☐ Anwalt ☒ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

Deutsche Telekom AG
Patentabteilung R151
64307 Darmstadt
Deutschland

Telefonnr.: 06151/83-58 42

Telefaxnr.: 06151/83-58 43

Fernschreibnr.:

☐ **Zustellanschrift:** Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

EL594612691

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

- ☐ **AP** **ARIPO-Patent:** **GH** Ghana, **GM** Gambia, **KE** Kenia, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SL** Sierra Leone, **SZ** Swasiland, **UG** Uganda, **ZW** Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☐ **EA** **Eurasisches Patent:** **AM** Armenien, **AZ** Aserbaidschan, **BY** Belarus, **KG** Kirgisistan, **KZ** Kasachstan, **MD** Republik Moldau, **RU** Russische Föderation, **TJ** Tadschikistan, **TM** Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ **EP** **Europäisches Patent:** **AT** Österreich, **BE** Belgien, **CH und LI** Schweiz und Liechtenstein, **CY** Zypern, **DE** Deutschland, **DK** Dänemark, **ES** Spanien, **FI** Finnland, **FR** Frankreich, **GB** Vereinigtes Königreich, **GR** Griechenland, **IE** Irland, **IT** Italien, **LU** Luxemburg, **MC** Monaco, **NL** Niederlande, **PT** Portugal, **SE** Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☐ **OA** **OAPI-Patent:** **BF** Burkina Faso, **BJ** Benin, **CF** Zentralafrikanische Republik, **CG** Kongo, **CI** Côte d'Ivoire, **CM** Kamerun, **GA** Gabun, **GN** Guinea, **GW** Guinea-Bissau, **ML** Mali, **MR** Mauretanien, **NE** Niger, **SN** Senegal, **TD** Tschad, **TG** Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

- ☐ **AE** Vereinigte Arabische Emirate
- ☐ **AL** Albanien .....
- ☐ **AM** Armenien .....
- ☐ **AT** Österreich .....
- ☐ **AU** Australien .....
- ☐ **AZ** Aserbaidschan
- ☐ **BA** Bosnien-Herzegowina .....
- ☐ **BB** Barbados
- ☐ **BG** Bulgarien .....
- ☐ **BR** Brasilien .....
- ☐ **BY** Belarus .....
- ☐ **CA** Kanada
- ☐ **CH und LI** Schweiz und Liechtenstein
- ☐ **CN** China .....
- ☐ **CU** Kuba .....
- ☐ **CZ** Tschechische Republik .....
- ☐ **DE** Deutschland .....
- ☐ **DK** Dänemark .....
- ☐ **EE** Estland .....
- ☐ **ES** Spanien .....
- ☐ **FI** Finnland .....
- ☐ **GB** Vereinigtes Königreich
- ☐ **GD** Grenada
- ☐ **GE** Georgien .....
- ☐ **GH** Ghana .....
- ☐ **GM** Gambia
- ☐ **HR** Kroatien .....
- ☒ **HU** Ungarn .....
- ☐ **ID** Indonesien
- ☒ **IL** Israel .....
- ☐ **IN** Indien .....
- ☐ **IS** Island
- ☒ **JP** Japan .....
- ☐ **KE** Kenia .....
- ☐ **KG** Kirgisistan .....
- ☐ **KP** Demokratische Volksrepublik Korea .....
- ☐ **KR** Republik Korea .....
- ☐ **KZ** Kasachstan .....
- ☐ **LC** Saint Lucia
- ☐ **LK** Sri Lanka
- ☐ **LR** Liberia
- ☐ **LS** Lesotho .....
- ☐ **LT** Litauen
- ☐ **LU** Luxemburg
- ☐ **LV** Lettland
- ☐ **MD** Republik Moldau .....
- ☐ **MG** Madagaskar .....
- ☐ **MK** Die ehemalige jugoslawische Republik Mazedonien .....
- ☐ **MN** Mongolei
- ☐ **MW** Malawi .....
- ☐ **MX** Mexiko .....
- ☐ **NO** Norwegen
- ☐ **NZ** Neuseeland .....
- ☐ **PL** Polen .....
- ☐ **PT** Portugal .....
- ☐ **RO** Rumänien
- ☐ **RU** Russische Föderation .....
- ☐ **SD** Sudan
- ☐ **SE** Schweden
- ☐ **SG** Singapur
- ☐ **SI** Slowenien .....
- ☐ **SK** Slowakei .....
- ☐ **SL** Sierra Leone .....
- ☐ **TJ** Tadschikistan .....
- ☐ **TM** Turkmenistan .....
- ☐ **TR** Türkei .....
- ☐ **TT** Trinidad und Tobago .....
- ☐ **UA** Ukraine .....
- ☐ **UG** Uganda .....
- ☒ **US** Vereinigte Staaten von Amerika .....
- ☐ **UZ** Usbekistan .....
- ☐ **VN** Vietnam .....
- ☐ **YU** Jugoslawien .....
- ☐ **ZA** Südafrika .....
- ☐ **ZW** Simbabwe .....

Kästchen für die Bestimmung von Staaten, die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☐ .....
- ☐ .....

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

Feld Nr. VI PRIORITÄTSANSPRUCH

☐ Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.

Anmeldedatum der früheren Anmeldung (Tag/Monat/Jahr)	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine: nationale Anmeldung: Staat	regionale Anmeldung:* regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) 09.Oktober 1998 (09.10.1998)	19847944.1	DE		
Zeile (2)				
Zeile (3)				

☐ Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben in der (den) Zeile(n) _____ bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln *(nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist(sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)*

* *Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, so muß in dem Zusatzfeld mindestens ein Staat angegeben werden, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung eingereicht wurde.*

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA) *(falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden):*

ISA / EP

Antrag auf Nutzung der Ergebnisse einer früheren Recherche; Bezugnahme auf diese frühere Recherche *(falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist):*

Datum *(Tag/Monat/Jahr)* Aktenzeichen Staat *(oder regionales Amt)*

Feld Nr. VIII KONTROLLISTE; EINREICHUNGSSPRACHE

Diese internationale Anmeldung enthält die folgende **Anzahl von Blättern:**

Antrag	: 4
Beschreibung (ohne Sequenzprotokollteil)	: 5
Ansprüche	: 1
Zusammenfassung	: 1
Zeichnungen	: —
Sequenzprotokollteil der Beschreibung	: —
Blattzahl insgesamt	: 11

Dieser internationalen Anmeldung **liegen** die nachstehend angekreuzten Unterlagen **bei:**

1. ☒ Blatt für die Gebührenberechnung
2. ☐ Gesonderte unterzeichnete Vollmacht
3. ☒ Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden): 38692
4. ☐ Begründung für das Fehlen einer Unterschrift
5. ☐ Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer gekennzeichnet:
6. ☐ Übersetzung der internationalen Anmeldung in die folgende Sprache:
7. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material
8. ☐ Protokoll der Nucleotid- und/oder Aminosäuresequenzen in computerlesbarer Form
9. ☐ Sonstige *(einzeln aufführen)*: Zusatzblatt 4

Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.):

Sprache, in der die internationale Anmeldung eingereicht wird: deutsch

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Deutsche Telekom AG

i.A.

..... Fortsetzung Blatt 4

Rolf Henn, Referent der Patentabteilung
EPA-Vollmacht 38692

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung: (22.09.99) 22 SEP 1999	2. Zeichnungen ☐ eingegangen: ☐ nicht eingegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:	
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:	
5. Internationale Recherchenbehörde *(falls zwei oder mehr zuständig sind)*: ISA /	6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Zusatzfeld *Wird dieses Zusatzfeld nicht benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.*

1. Wenn der ***Platz in einem Feld nicht für alle Angaben ausreicht****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. ...." [Nummer des Feldes angeben] und machen die Angaben entsprechend der in dem Feld, in dem der Platz nicht ausreicht, vorgeschriebenen Art und Weise, insbesondere:*

(i) ***Wenn mehr als zwei Anmelder und/oder Erfinder vorhanden sind*** *und kein "Fortsetzungsblatt" zur Verfügung steht: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. III" und machen für jede weitere Person die in Feld Nr. III vorgeschriebenen Angaben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.*

(ii) Wenn in Feld Nr. II oder III die Angabe ***"die im Zusatzfeld angegebenen Staaten"*** *angekreuzt ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Anmelders oder die Namen der Anmelder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Anmelder ist.*

(iii) Wenn der in Feld Nr. II oder III genannte ***Erfinder oder Erfinder/Anmelder nicht für alle Bestimmungsstaaten oder für die Vereinigten Staaten von Amerika als Erfinder benannt ist****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Erfinders oder die Namen der Erfinder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Erfinder ist.*

(iv) Wenn zusätzlich zu dem Anwalt oder den Anwälten, die in Feld Nr. IV angegeben sind, ***weitere Anwälte*** *bestellt sind: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. IV" und machen für jeden weiteren Anwalt die entsprechenden, in Feld Nr. IV vorgeschriebenen Angaben.*

(v) Wenn in Feld Nr. V bei einem Staat (oder bei OAPI) die Angabe ***"Zusatzpatent"*** *oder* ***"Zusatzzertifikat,"*** *oder wenn in Feld Nr. V bei den Vereinigten Staaten von Amerika die Angabe* ***"Fortsetzung"*** *oder* ***"Teilfortsetzung"*** *hinzugefügt wird: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. V" und geben den Namen des betreffenden Staats (oder OAPI) an und nach dem Namen jedes solchen Staats (oder OAPI) das Aktenzeichen des Hauptschutzrechts oder der Hauptschutzrechtsanmeldung und das Datum der Erteilung des Hauptschutzrechts oder der Einreichung der Hauptschutzrechtsanmeldung.*

(vi) Wenn in Feld Nr. VI ***die Priorität von mehr als drei früheren Anmeldungen beansprucht wird****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und machen für jede weitere frühere Anmeldung die entsprechenden, in Feld Nr. VI vorgeschriebenen Angaben.*

(vii) Wenn in Feld Nr. VI die ***frühere Anmeldung eine ARIPO Anmeldung*** *ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und geben, unter Angabe der Nummer der Zeile, in der die die frühere Anmeldung betreffenden Angaben gemacht sind, mindestens einen Staat an, der Mitglied der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung erfolgte.*

2. Wenn, im Hinblick auf die ***Erklärung bzgl. vorsorglicher Bestimmungen*** *in Feld Nr. V, der Anmelder Staaten von dieser Erklärung ausnehmen möchte: In diesem Fall schreiben Sie "Bestimmung(en), die von der Erklärung bzgl. vorsorglicher Bestimmungen ausgenommen ist(sind)" und geben den Namen oder den Zweibuchstaben-Code jedes so ausgeschlossenen Staates an.*

3. Wenn der Anmelder für irgendein Bestimmungsamt die Vorteile nationaler Vorschriften betreffend ***unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit*** *in Anspruch nimmt: In diesem Fall schreiben Sie "Erklärung betreffend unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit" und geben im folgenden die entsprechende Erklärung ab.*

M/ef Fortsetzung von Feld Nr IX

Die Unterschrift des Erfinders bzw. Anmelders und die Prioritätsbescheinigung wird nachgereicht.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
P98135WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/07052	22/09/1999	09/10/1998
Anmelder		
DEUTSCHE TELEKOM AG ET AL		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

   [X] keine der Abb.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/07052

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	LAIH C -S ET AL: "On the design of conference key distribution systems for the broadcasting networks" IEEE INFOCOM ' 93. THE CONFERENCE ON COMPUTER COMMUNICATIONS PROCEEDINGS. TWELFTH ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES. NETWORKING: FOUNDATION FOR THE FUTURE (CAT. NO.93CH3264-9), 28. März 1993 (1993-03-28) - 1. April 1993 (1993-04-01), Seiten 1406-1413 vol.3, XP000419708 Los Alamitos, CA, USA, IEEE Comput. Soc. Press, USA ISBN: 0-8186-3580-0 Seite 1409, Spalte 2, letzter Absatz -Seite 1410, Spalte 1 --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
29. Dezember 1999	24/01/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

1

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 768 773 A (DEUTSCHE TELEKOM AG) 16. April 1997 (1997-04-16) in der Anmeldung erwähnt Spalte 2, Zeile 23 -Spalte 3, Zeile 22 ---	1
A	STEINER M ET AL: "Diffie-Hellman key distribution extended to group communication" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14. - 16. März 1996, Seiten 31-37, XP000620975 New York, NY, USA, ACM ISBN: 0-89791-829-0 in der Anmeldung erwähnt Seite 34 ---	1
A	BURMESTER M ET AL: "A secure and efficient conference key distribution system" ADVANCES IN CRYPTOLOGY - EUROCRYPT '94. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, PROCEEDINGS OF EUROCRYPT '94, PERUGIA, ITALY, 9-12 MAY 1994, Seiten 275-286, XP000852509 1995, Springer-Verlag, Germany ISBN: 3-540-60176-7 in der Anmeldung erwähnt Seite 277, letzter Absatz -Seite 282 ---	1
A	DIFFIE W ET AL: "New directions in cryptography" IEEE TRANSACTIONS ON INFORMATION THEORY, NOV. 1976, USA, Bd. IT-22, Nr. 6, Seiten 644-654, XP000565260 ISSN: 0018-9448 in der Anmeldung erwähnt Seite 647, Spalte 2 -Seite 649 -----	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 99/07052

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0768773 A	16-04-1997	DE 19538385 A	17-04-1997
		AT 186432 T	15-11-1999
		AU 6572796 A	17-04-1997
		CA 2181972 A	15-04-1997
		DE 59603557 D	09-12-1999
		NO 962672 A	15-04-1997
		NZ 299014 A	24-09-1998
		US 5903649 A	11-05-1999

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/07052

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LAIH C -S ET AL: "On the design of conference key distribution systems for the broadcasting networks" IEEE INFOCOM ' 93. THE CONFERENCE ON COMPUTER COMMUNICATIONS PROCEEDINGS. TWELFTH ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES. NETWORKING: FOUNDATION FOR THE FUTURE (CAT. NO.93CH3264-9), 28 March 1993 (1993-03-28) - 1 April 1993 (1993-04-01), pages 1406-1413 vol.3, XP000419708 Los Alamitos, CA, USA, IEEE Comput. Soc. Press, USA ISBN: 0-8186-3580-0 page 1409, column 2, last paragraph -page 1410, column 1 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

' Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 December 1999	24/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Zucka, G

Form PCT/ISA/210 (second sheet) (July 1992)

EL594612691

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 768 773 A (DEUTSCHE TELEKOM AG) 16 April 1997 (1997-04-16) cited in the application column 2, line 23 -column 3, line 22 ---	1
A	STEINER M ET AL: "Diffie-Hellman key distribution extended to group communication" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14 - 16 March 1996, pages 31-37, XP000620975 New York, NY, USA, ACM ISBN: 0-89791-829-0 cited in the application page 34 ---	1
A	BURMESTER M ET AL: "A secure and efficient conference key distribution system" ADVANCES IN CRYPTOLOGY - EUROCRYPT '94. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, PROCEEDINGS OF EUROCRYPT '94, PERUGIA, ITALY, 9-12 MAY 1994, pages 275-286, XP000852509 1995, Springer-Verlag, Germany ISBN: 3-540-60176-7 cited in the application page 277, last paragraph -page 282 ---	1
A	DIFFIE W ET AL: "New directions in cryptography" IEEE TRANSACTIONS ON INFORMATION THEORY, NOV. 1976, USA, vol. IT-22, no. 6, pages 644-654, XP000565260 ISSN: 0018-9448 cited in the application page 647, column 2 -page 649 -----	1

INTERNATIONAL SEARCH REPORT

[redacted]rmation on patent family members

[redacted]onal Application No
PCT/EP 99/07052

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0768773 A	16-04-1997	DE 19538385 A	17-04-1997
		AT 186432 T	15-11-1999
		AU 6572796 A	17-04-1997
		CA 2181972 A	15-04-1997
		DE 59603557 D	09-12-1999
		NO 962672 A	15-04-1997
		NZ 299014 A	24-09-1998
		US 5903649 A	11-05-1999

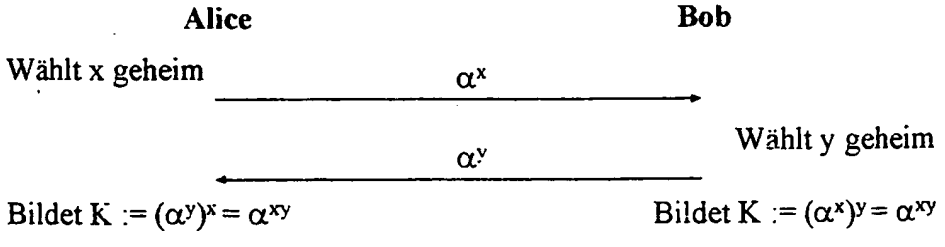
Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern

Beschreibung:

Die Erfindung betrifft ein Verfahren zum Etablieren eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von Teilnehmern gemäß dem Oberbegriff des unabhängigen Anspruchs. Verschlüsselungsverfahren in vielfältiger Art gehören zum Stand der Technik und haben zunehmend kommerzielle Bedeutung. Sie werden dazu eingesetzt, Nachrichten über allgemein zugängliche Übertragungsmedien zu übertragen, wobei aber nur die Besitzer eines Krypto-Schlüssels diese Nachrichten im Klartext lesen können.

Ein bekanntes Verfahren zur Etablierung eines gemeinsamen Schlüssels über unsichere Kommunikationskanäle ist z. B. das Verfahren von W. Diffie und W. Hellmann (siehe DH-Verfahren W. Diffie und M. Hellmann, siehe New Directions in Cryptography, IEEE Transaction on Information Theory, IT-22(6):644-654, November 1976)

Grundlage des DH-Schlüsselaustauschs [DH76] ist die Tatsache, daß es praktisch unmöglich ist, Logarithmen modulo einer großen Primzahl p zu berechnen. Dies machen sich Alice und Bob in dem unten abgebildeten Beispiel zunutze, indem sie jeweils eine Zahl x bzw. y kleiner als p (und teilerfremd zu p-1) geheim wählen. Dann senden sie sich (nacheinander oder gleichzeitig) die x-te (bzw. y-te) Potenz einer öffentlich bekannten Zahl α zu. Aus den empfangenen Potenzen können sie durch erneutes Potenzieren mit x bzw. y einen gemeinsamen Schlüssel $K:=\alpha^{xy}$ berechnen. Ein Angreifer, der nur α^x und α^y sieht, kann daraus K nicht berechnen. (Die einzige heute bekannte Methode dazu bestünde darin, zunächst den Logarithmus z.B. von α^x zur Basis α modulo p zu berechnen, und dann α^y damit zu potenzieren.)



Beispiel für Diffie-Hellman-Schlüsselaustausch

Das Problem beim DH-Schlüsselaustausch besteht darin, daß Alice nicht weiß, ob sie tatsächlich mit Bob kommuniziert, oder mit einem Betrüger. In IPSec wird dieses Problem durch den Einsatz von Public-Key-Zertifikaten gelöst, in denen durch eine vertrauenswürdige Instanz die Identität eines Teilnehmers mit einem öffentlichen Schlüssel verknüpft wird. Dadurch wird die Identität eines Gesprächspartners überprüfbar.

Der DH-Schlüsselaustausch kann auch mit anderen mathematischen Strukturen realisiert werden, z.B. mit endlichen Körpern $GF(2^n)$ oder Elliptischen Kurven. Mit diesen Alternativen kann man die Performance verbessern.

Dieses Verfahren ist allerdings nur zur Vereinbarung eines Schlüssels zwischen zwei Teilnehmern geeignet.

Es wurden verschiedene Versuche unternommen, das DH-Verfahren auf drei oder mehr Teilnehmer zu erweitern (Gruppen DH). Einen Überblick über den Stand der Technik bietet M. Steiner, G.Tsudik, M. Waidner, in Diffie-Hellmann Key Distribution Extended to Group Communication, Proc. 3rd ACM Conference on Computer and Communicatios Security, März 1996, Neu Delhi, Indien.

Eine Erweiterung des DH-Verfahrens auf Teilnehmer A, B und C wird z.B. durch nachfolgende Tabelle beschrieben (Berechnungen jeweils mod p):

	$A \rightarrow B$	$B \rightarrow C$	$C \rightarrow A$
1. Runde	g^a	g^b	g^c
2. Runde	g^{ca}	g^{ab}	g^{bc}

Nach Durchführung dieser beiden Runden kann jeder der Teilnehmer den geheimen Schlüssel g^{abc} mod p berechnen.

Bei allen diesen Erweiterungen tritt mindestens eines der folgenden Probleme auf:

- Die Teilnehmer müssen in einer bestimmten Art und Weise geordnet sein, im obigen Beispiel z.B. als Kreis.
- Die Teilnehmer haben gegenüber der Zentrale keinen Einfluß auf die Auswahl des Schlüssels.
- Die Rundenzahl ist abhängig von der Teilnehmerzahl.

Diese Verfahren sind in der Regel schwer zu implementieren und sehr rechenaufwendig.

Ein weiteres Verfahren zum gemeinsamen Etablieren eines Schlüssels ist aus DE 195 38 385.0 bekannt. Bei diesem Verfahren muß die Zentrale allerdings die geheimen Schlüssel der Teilnehmer kennen.

Weiterhin ist eine Lösung aus Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 bekannt, bei der zwei Runden zur Generierung des Schlüssels benötigt werden, wobei in der zweiten Runde durch die Zentrale für n Teilnehmer n Nachrichten der Länge p = ca. 1000Bit gesendet werden müssen.

Bekannt ist auch ein als (n,t)-Threshold-Verfahren bezeichnetes kryptographisches Verfahren. Mit einem (n,t)-Threshold-Verfahren kann man einen Schlüssel k so in t Teile, die shadows genannt werden, zerlegen, daß dieser Schlüssel k aus je n der t shadows rekonstruiert werden kann (vgl. Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie (2. Auflage), Vieweg Verlag, Wiesbaden 1998).

Das vorliegende Verfahren zur Erzeugung eines gemeinsamen Schlüssels zwischen einer Zentrale und einer Gruppe von mindestens drei Teilnehmern soll den gleichen Sicherheitsstandard wie das DH-Verfahren aufweisen. Das Verfahren soll dabei jedoch einfach zu implementieren sein und einen minimalen Rechenaufwand benötigen. Das Verfahren soll so ausgebildet sein, daß die geheimen Schlüssel der Teilnehmer der Zentrale dabei nicht bekannt gemacht werden müssen.

Das erfindungsgemäße Verfahren, das dieser Aufgabenstellung gerecht wird, basiert auf den gleichen mathematischen Strukturen, wie das DH-Verfahren und weist daher vergleichbare Sicherheitsmerkmale auf. Im Vergleich zu den bisher vorgeschlagenen Gruppen-DH-Verfahren ist es wesentlich effizienter im Hinblick auf Rechenaufwand und Kommunikationsbedarf.

Nachfolgend wird das Wirkprinzip des erfindungsgemäßen Verfahrens näher erläutert. Die Zentrale wird dabei mit Z bezeichnet, definierte Teilnehmer am Verfahren mit T1-Tn und jeder einzelne nicht konkret benannte Teilnehmer mit Ti. Die öffentlich bekannten Komponenten des Verfahrens sind eine öffentlich bekannte mathematische Gruppe G,

vorzugsweise die multiplikative Gruppe aller ganzen Zahlen modulo einer großen Primzahl p, und ein Element g der Gruppe G, vorzugsweise eine Zahl $0<g<p$ mit großer multiplikativer Ordnung. Für die Gruppe G können jedoch auch andere geeignete mathematische Strukturen verwendet werden, z.B. die multiplikative Gruppe eines endlichen Körpers, oder die Gruppe der Punkte einer elliptischen Kurve.

Das Verfahren verläuft in drei Arbeitsschritten.

Im ersten Arbeitsschritt wird von jedem Teilnehmer Ti eine Nachricht der Form (Ti, g^i mod p) an die Zentrale gesendet, wobei i eine mittels eines Zufallsgenerators gewählte zufällige Zahl des Teilnehmers Ti ist.

Im zweiten Arbeitsschritt wird in der Zentrale Z

- eine zufällige Zahl z generiert und für jeden Teilnehmer Ti die Zahl $(g^i)^z$ mod p berechnet.
- Bei n Teilnehmern werden in der Zentrale Z dann aus diesen n Zahlen n shares mit Hilfe eines an sich bekannten (n, 2n-1) Threshold Verfahrens abgeleitet.
- In der Zentrale Z werden n-1 weitere shares s^1-s^{n-1} ausgewählt und zusammen mit der Zahl g^z mod p an alle Teilnehmer T1-Tn gesendet.

Im dritten Arbeitsschritt wird bei jedem Teilnehmer Ti der gemeinsamen Schlüssel k berechnet, wobei

- $(g^z)^i$ mod p = $(g^i)^z$ mod p berechnet wird,
- daraus ein share des Threshold Verfahrens abgeleitet wird und
- mit diesem share und $s^1,...s^{n-1}$ als Geheimnis der gemeinsame Schlüssel k ermittelt wird.

Nachfolgend wird das erfindungsgemäße Verfahren anhand eines konkreten Beispiels für drei Teilnehmer A, B, und C sowie einer Zentrale Z näher erläutert. Die Anzahl der Teilnehmer ist jedoch auf beliebig viele Teilnehmer erweiterbar.

Bei diesem Beispiel beträgt die Länge der Zahl p 1024 Bit; g hat eine multiplikative Ordnung von mindestens 2^{160}.

Das erfindungsgemäße Verfahren läuft nach folgenden Verfahrensschritten ab:

1. Teilnehmer A, B und C senden g^a mod p, g^b mod p und g^c mod p an die Zentrale Z.
2. In der Zentrale Z wird g^{az} mod p, g^{bz} mod p und g^{cz} mod p berechnet, wobei jeweils die 128 Least Significant Bits davon als shares s_A, s_B bzw. s_C verwendet werden. In der Zentrale Z wird mittels des (n,2,-1)-Threshold-Verfahrens ein Polynom P(x) über einem endlichen Körper GF(2^{128}) vom Grad 2 berechnet, das durch die Punkte $(1,s_A)$, $(2,s_B)$ und $(3,s_C)$ geht und durch diese eindeutig festgelegt ist. Der gemeinsame Schlüssel k ist der Schnittpunkt dieses Polynoms mit der y-Achse, d. h. k; =P(0). Die Zentrale Z sendet nun g^z mod p, s_1;=P(4) und s_2;=P(5) an die Teilnehmer A, B und C.
3. Beim Teilnehmer A wird $(g^z)^a$ mod p berechnet. Im Ergebnis erhält der Teilnehmer A mit den 128 Least Significant Bits dieses Wertes den share s_A, der zusammen mit den shares s_1 und s_2 ausreicht, das Polynom P´(x) und damit auch den Schlüssel k zu bestimmen. Bei den Teilnehmern B und C wird analog verfahren.

Das oben beschriebene Verfahren kommt mit der minimalen Anzahl von zwei Runden zwischen den Teilnehmern T1-Tn und Zentrale Z aus. In der zweiten Runde kann der Aufwand für die von der Zentrale an die n Teilnehmer zu übertragenden Zeichenfolgen im Gegensatz zu der Lösung von Burmester und Desmedt auf eine Länge von jeweils 128 Bit pro Teilnehmer reduziert werden.

(1) Patentanspruch:

1. Verfahren zum Etablieren eines gemeinsamen Schlüssels k zwischen einer Zentrale Z und einer Gruppe von Teilnehmern T1-Tn mit einer öffentlich bekannten mathematischen Gruppe G und einem Element $g \in G$ von großer Ordnung in der Gruppe G, so daß für die Gruppe G und das Element g die Berechnung des diskreten Logarithmus praktisch unmöglich ist, **dadurch gekennzeichnet**, daß

a) von jedem Teilnehmer (Ti) eine Zufallszahl (i) generiert und aus dem bekannten Element $g \in G$ und der jeweiligen Zufallszahl (i) von jedem Teilnehmer (Ti) der Wert (g^i) berechnet und zur Zentrale (Z) gesendet wird, daß

b) in der Zentrale (Z) eine Zufallszahl (z) generiert wird, daß aus der Zufallszahl (z) und den empfangenen Werten(g^i) die Werte $(g^i)^z$ in G berechnet werden, daß aus diesen Werten n shares $(s_1,...,s_n)$ eines Threshold-Verfahrens abgeleitet werden , und daß aus den shares $(s_1,...,s_n)$ ein (n,2,-1)-Threshold-Verfahren konstruiert wird, wobei das durch dieses Verfahren implizid gegebene Geheimnis der zu etablierende Schlüssel (k) ist, daß in der Zentrale (Z) n-1 weitere, von den shares $(s_1,...,s_n)$ verschiedene shares $(s_{n+1},...s_{2n-1})$ zusammen mit dem Wert g^z in G berechnet und an die Teilnehmer (T1-Tn) übertragen werden, und daß

c) bei jedem Teilnehmer (Ti) der zu etablierende Schlüssel (k) dadurch rekonstruiert wird, daß aus dem von der Zentrale (Z) übertragenen Wert (g^z) und der Zufallszahl (i) des jeweiligen Teilnehmers (Ti) der Wert für $(g^z)^i$ in G berechnet wird, daß aus dem resultierenden Wert mittels eines Threshold Verfahrens der share (s_i) abgeleitet wird und daß mit dem share (s_i) und den von der Zentrale (Z) übertragenen shares $(s_{n+1},...s_{2n-1})$ mit Hilfe des (n,2,-i)-Threshold-Verfahrens der Schlüssel (k) rekonstruiert wird.